Thüringen auf dem Weg in die Informationsgesellschaft

Sicherheit mobiler Kommunikation

Bauhaus-Universität Weimar, Fakultät Medien
bernd.schalbe@medien.uni-weimar.de
www.uni-weimar.de/medien

Bauhaus-Universität Weimar
fakultät medien [faculty of media]

Inhalt

- Sicherheit im allgemeinen
- Sicherheit in mobilen Umgebungen
- mobile Telephonie – GSM
- drahtlose Netze – WLAN
- Lösungsansätze
- Fazit

Sicherheitsziele

Sicherheit ist zentrales Grundbedürfnis – besonders bei Datenübertragung in Netzwerken

- Vertraulichkeit (privacy)
  übertragene Daten sollen für Dritte nicht lesbar sein
- Authentizität (authenticity)
  Identität der Kommunikationspartner muss zweifelsfrei sein
  Einem Dritten soll es nicht möglich sein, unerkannt Daten in eine Verbindung einzuschleusen
- Integrität (integrity)
  ausgetauschte Daten sollen nicht unerkannt durch Dritte verändert werden können

Sicherheitsziele

Weitere Sicherheitsziele

- Nicht-Anfechtbarkeit (non-repudiation)
  Absender soll den Versand einer Nachricht später nicht leugnen können
- Zugriffssteuerung (access control)
  die Infrastruktur und die Dienste sollen gegen die Benutzung durch Unbefugte geschützt sein
- Verfügbarkeit (availability)
  es muss sichergestellt werden, dass Dienste bei Bedarf auch verfügbar sind

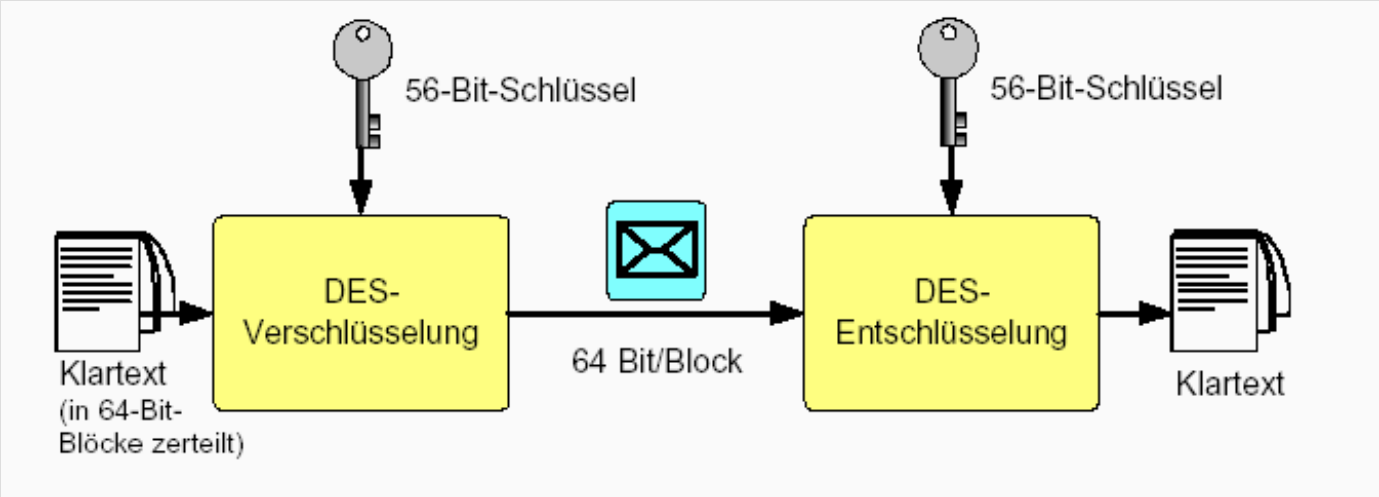
Kryptografie

Die genannten Sicherheitsziele lassen sich durch den Einsatz von Verschlüsselung erreichen

- Vertraulichkeit
  ohne Kenntnis des Schlüssels können Dritte die Daten nicht lesen
- Symmetrische Verschlüsselung
  beide Partner benutzen einen geheimen Schlüssel
  der geheime Schlüssel muss über einen sicheren Kanal übertragen werden bzw. vorhanden sein
- Asymmetrische Verschlüsselung
  Schlüsselpaar – privater und öffentlicher Schlüssel
  es ist kein sicherer Kanal notwendig

Symmetrische Verschlüsselung - DES

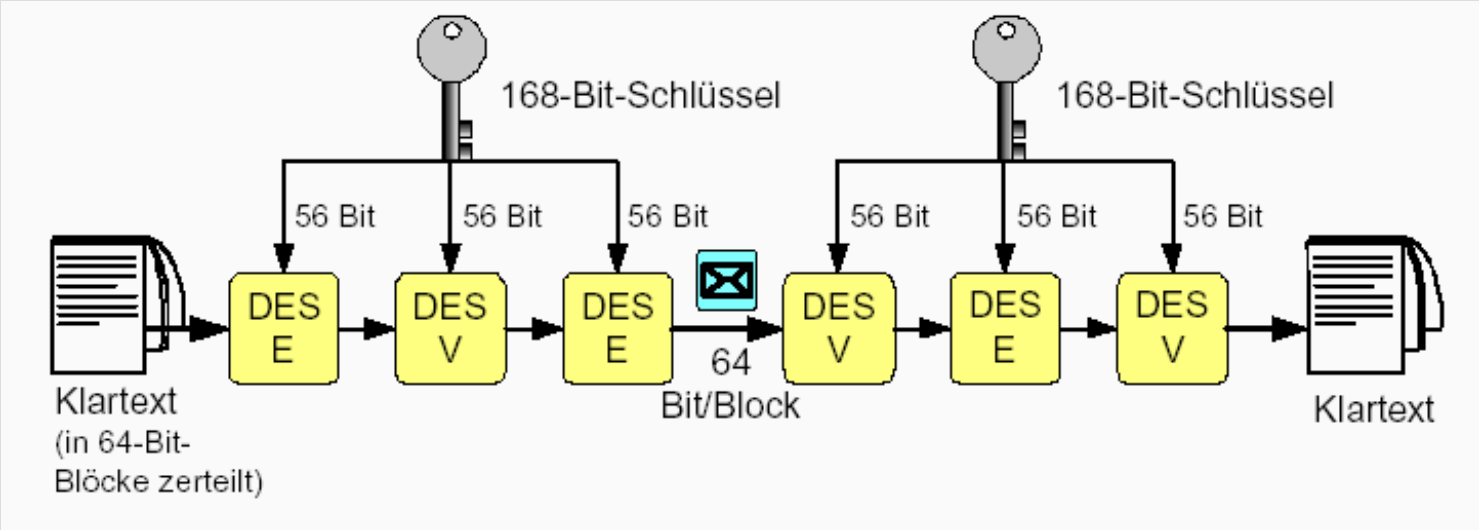
DES – Data Encryption Standard



- seit 1977
- Permutation – 16 x Rotation – S-Boxen – Permutation
- bisher nicht gebrochen
- 56-Bit Schlüssel anfällig gegen Brute Force Attacken

Symmetrische Verschlüsselung - TDEA

TDEA – Triple Data Encryption Algorithm

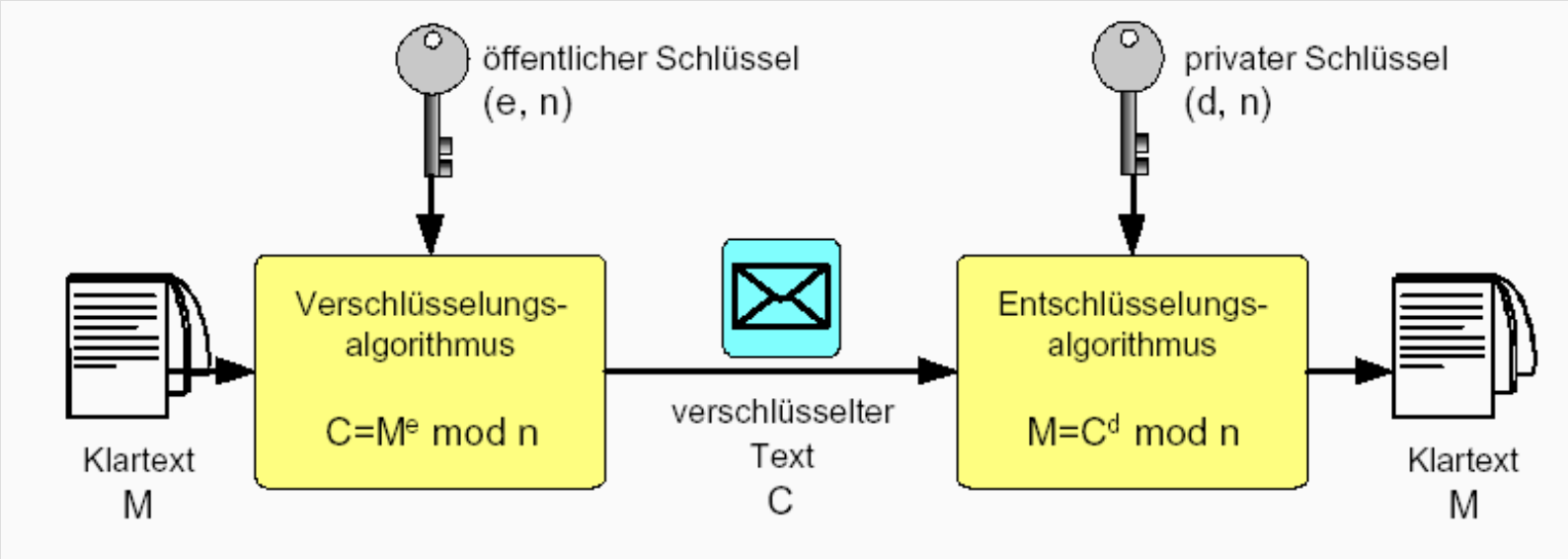


- seit 1979
- intern 3 mal DES (gleicher Algorithmus und Hardware)
- 168 Bit-Schlüssel -> Brute Force braucht 10^{31} Jahre bei einer Rechnerleistung von 10^{12} Entschlüsselungen/s

1997 AES -> 2000 Riijndael -> erster Makel in 2002

Asymmetrische Verschlüsselung - RSA

RSA – Rivest, Shamir, Adleman



- d, e, n werden aus zwei Primzahlen generiert
- die Primzahlen sollten sehr groß sein (> 1024 Bit)
- Komplexität der Primfaktorzerlegung ist der Sicherheitsfaktor

Hashfunktionen

- Hashfunktionen bilden aus einem Datenblock x einen Wert h fester Größe
- bei einer idealen Hashfunktion ist es unmöglich, dass zu einem Hashwert mehr als ein Datenblock existiert
- aus dem Hashwert sind unmöglich Informationen über den Datenblock abzuleiten
- Beispiele sind
  - SHA-1
    160 Bit Hashwert aus bis zu 2 Millionen Terabyte
  - MD5
    128 Bit Hashwert aus einer beliebigen Anzahl von 512 Bit langen Blöcken

Womit betreiben wir mobile Kommunikation ?

Sprachliche Kommunikation

Mobiltelefone – GSM, UMTS

Datenorientierte Kommunikation

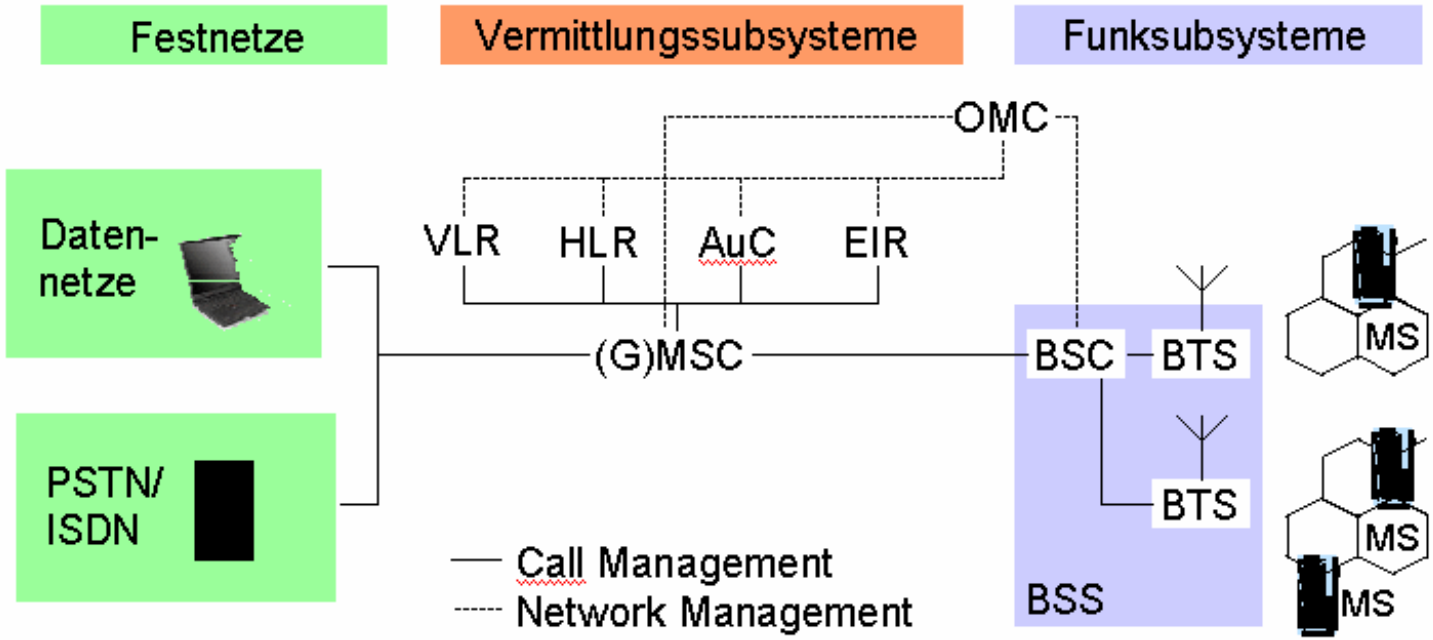
Mobiltelefone – GSM (GPRS), UMTS

mobiler Rechner (Notebook, PDA)
- WLAN (802.11), Bluetooth

Sicherheit bei mobiler Kommunikation

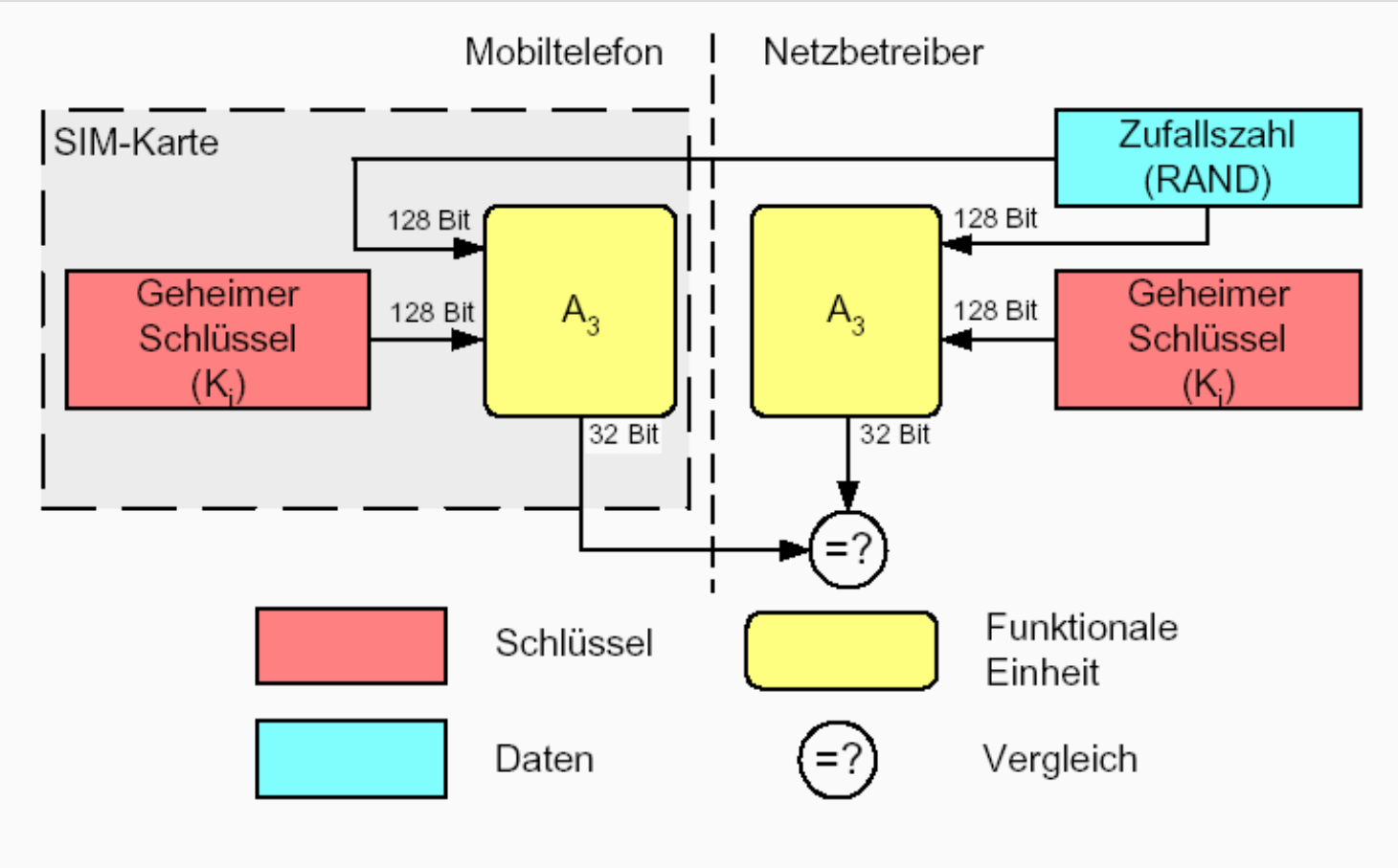
- mobile Umgebungen sind bedingt durch die Funkübertragung (Luftschnittstelle) prinzipiell unsicherer als drahtgebundene
- Sicherheitsziele:
  - vermeiden von unerlaubten Mithören
  - Erkennung der Verfälschung von Nachrichten
  - Benutzung nur für authentifizierte Benutzer und Geräte erlaubt
  - eindeutige, benutzerorientierte Kostenabrechnung
  - Vermeidung der einfachen Erstellung von Bewegungsprofilen

GSM: Struktur

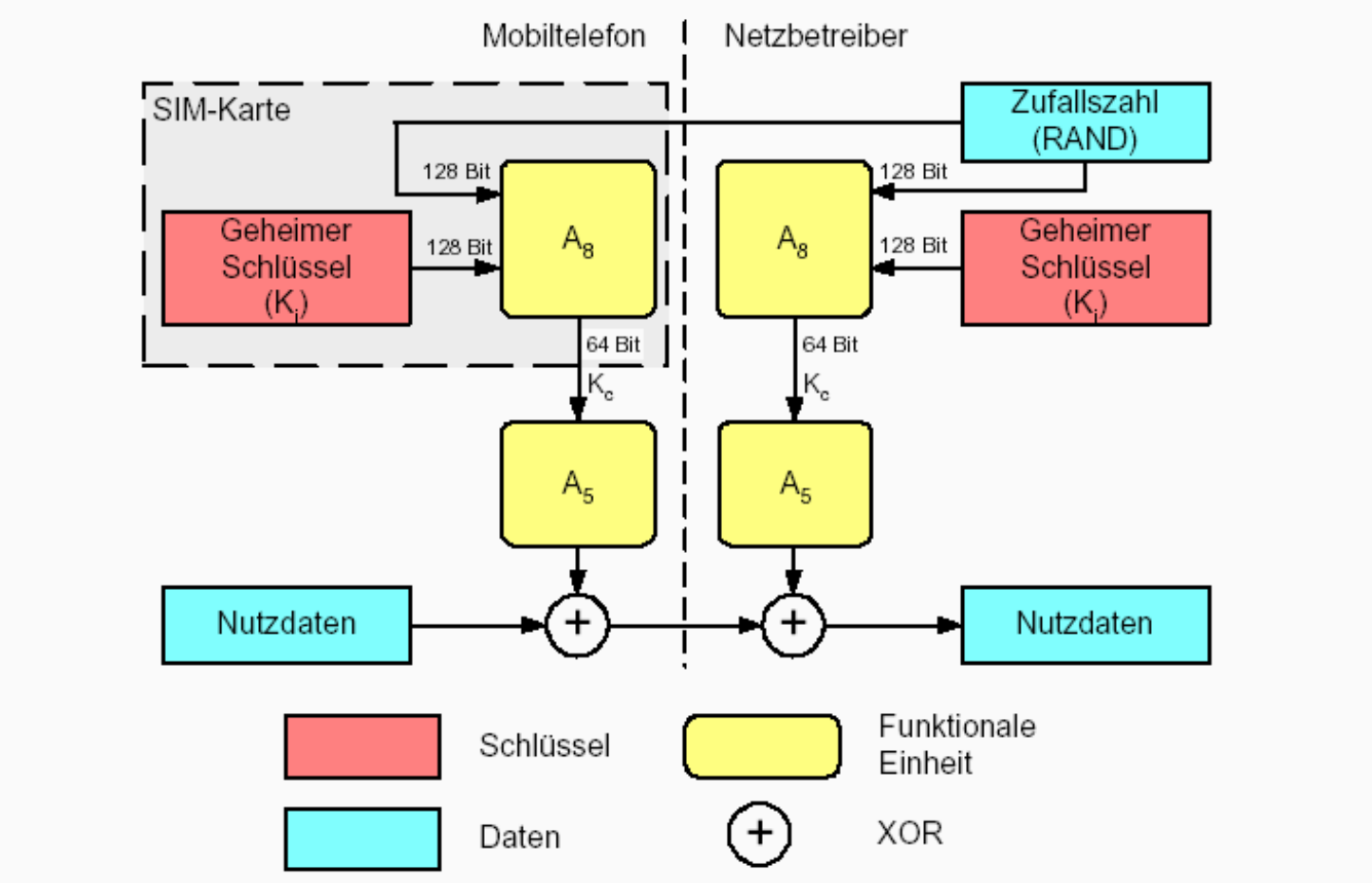


AuC	Authentication Centre	MS	Mobile Station
BSS	Base Station Subsystem	(G)MSC	(Gateway) Mobile Switching Centre
BSC	Base Station Controller	OMC	Operation and Maintenance Centre
BTS	Base Transceiver Station	PSTN	Public Switched Telephone Network
EIR	Equipment Identity Register	VLR	Visitor Location Register
HLR	Home Location Register	ISDN	Integrated Services Digital Network

GSM - Authentifizierung



GSM - Verschlüsselung



GSM – Anonymität der Benutzer

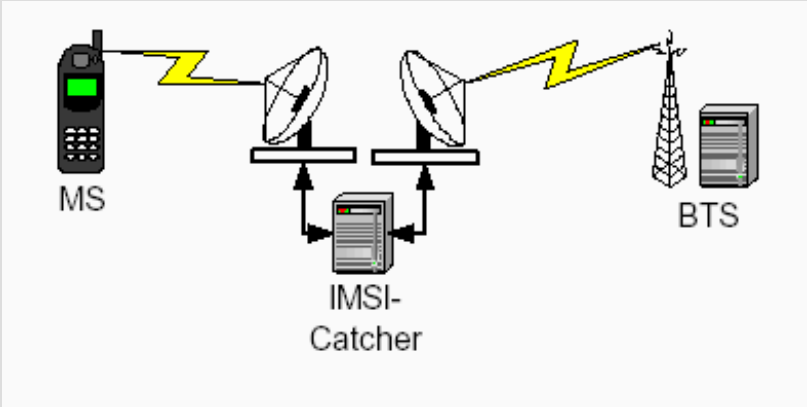
- beim ersten Einbuchen wird die IMSI übertragen, bei weiteren Einbuchungen die TMSI
- AuC ermittelt K_i
- um ein abhören zu erschweren, generiert AuC eine TMSI, die im HLR und in der SIM gespeichert wird

GSM - Sicherheitskritik

- A3, A5 und A8 wurden nicht veröffentlicht (security through obscurity)
- heutzutage ist man der Meinung, eine sichere Funktion sollte auch veröffentlicht werden
- A5 konnte mittlerweile rekonstruiert werden
- A3 und A8 gelten als unsicher
  durch wiederholte Authentisierungsanfragen kann K_i ermittelt werden -> duplizieren von SIM-Karten
- K_c nur 64 Bit -> Brute-Force realistisch

GSM - Sicherheitskritik

- Authentifizierung nur One-Way
  Basisstationen müssen sich nicht authentifizieren
- ein anderer Sender (IMSI-Catcher) könnte sich einklinken -> man-in-the-middle-attack



GSM - Sicherheitskritik

- der IMSI-Catcher kann IMSI und IMEI ermitteln
  -> dies erlaubt die Erstellung von Bewegungsprofilen
- noch schlimmer:
  der IMSI-Catcher kann das Mobiltelefon anweisen, die Verschlüsselung auszuschalten
- nun kann der IMSI-Catcher alle Telefonate abhören

GSM - Sicherheitskritik

Sicherheitsziele:

- vermeiden von unerlaubten Mithören
  nicht erfüllt
- Erkennung der Verfälschung von Nachrichten
  ???
- Benutzung nur für authentifizierte Benutzer und Geräte erlaubt
  nicht erfüllt
- eindeutige, benutzerorientierte Kostenabrechnung
  nicht erfüllt
- Vermeidung der einfachen Erstellung von Bewegungsprofilen
  nicht erfüllt

lesenswert:
GSM-Mobilfunk – Gefährdungen und Sicherheitsmaßnahme
BSI, Bonn 2003, http://www.bsi.bund.de

WLAN - Sicherheit

- drahtlose lokale Netze sind vermehrt Ziel von Angriffen
- der Netzbetreiben strebt mindestens das Sicherheitsniveau eines drahtgebundenen Netzes an
- die Norm IEEE 802.11 bietet drei Mechanismen an
  - Zugriffslisten
  - Authentifizierung
  - Verschlüsselung

WLAN - Zugriffslisten

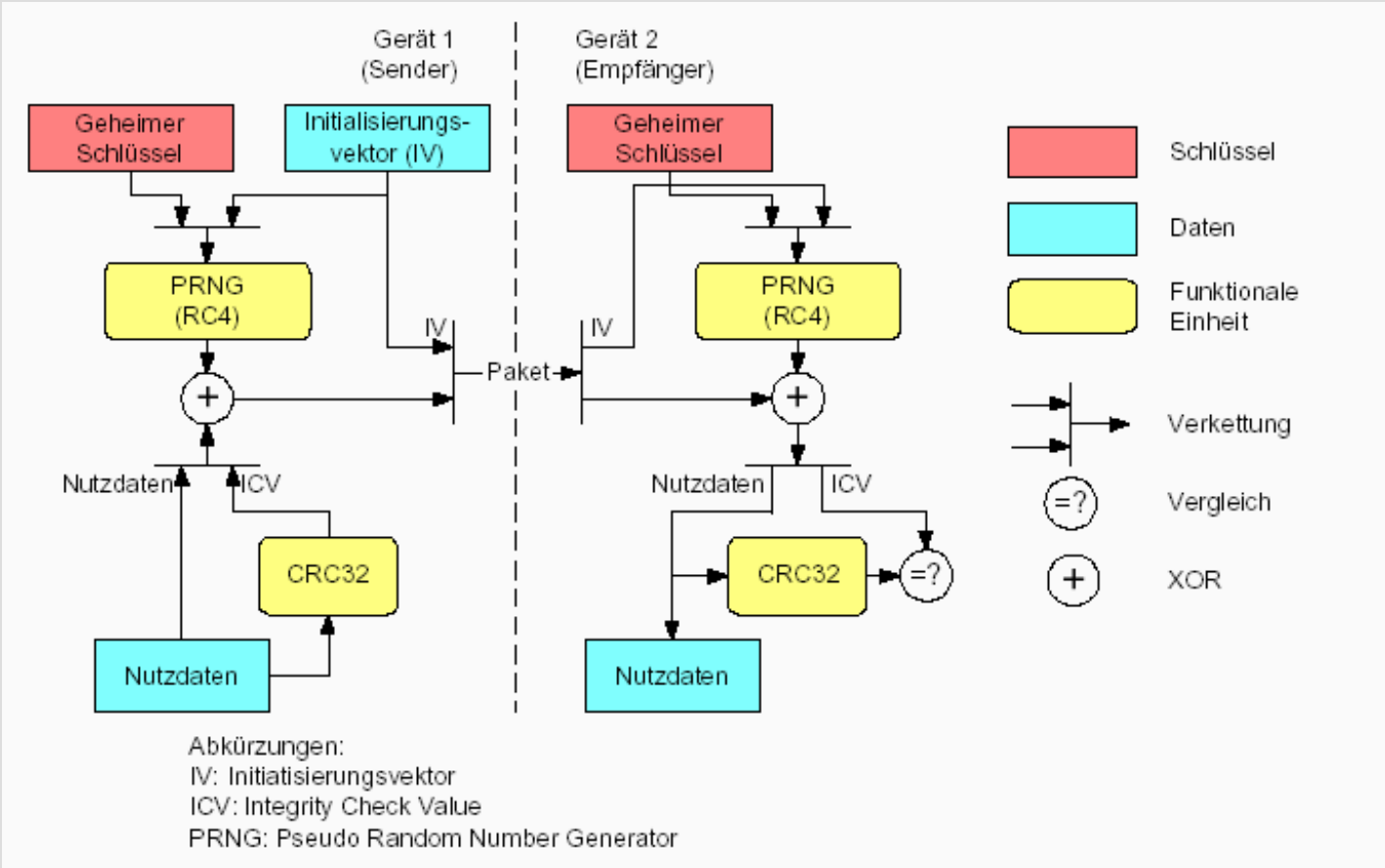
- Liste mit MAC-Adressen, die im Netz zulässig sind
  verwaltet pro Access-Point
- Nachteile
  - aufwendige manuelle Verwaltung
  - MAC-Adressen lassen sich einfach fälschen
  - MAC-Adressen können einfach abgehört werden

-> Zugriffslisten sind nicht sicher

WLAN – WEP (Wired Equivalent Privacy)

- jeder Access-Point und jede Station erhält gleichen geheimen Schlüssel
- symmetrische Verschlüsselung mit auf dem Schlüssel basierender Pseudo-Zufallsfolge
- Schlüssel erweitert um variablen Anteil (IV)
- zwei Schlüssellängen
  - 40 Bit Schlüssel, 24 Bit IV -> 40 Bit Verschlüsselung
  - 104 Bit Schlüssel, 24 Bit IV -> 128 Bit Verschlüsselung

WLAN – WEP-Verschlüsselung



WLAN (WEP) - Sicherheitskritik

- Ein Schlüssel für das gesamte Netz ist problematisch besonders in Hot Spots, wo die Vertrauenswürdigkeit der Benutzer nicht sichergestellt werden kann
- 40 Bit-Schlüssel sind zu klein
- der Algorithmus RC4 ist nicht mehr sicher
  es sind so genannte schwache Schlüssel bekannt, die es erlauben, bei Kenntnis nur einiger Schlüsselbits auf die gesamte Ausgabe zu schließen
- das CRC-Verfahren ist ungeeignet, um die Integrität von Paketen zu gewährleisten

-> WEP ist unsicher

WLAN - Sicherheitskritik

Sicherheitsziele:

- vermeiden von unerlaubten Mithören
  nicht erfüllt
- Erkennung der Verfälschung von Nachrichten
  nicht erfüllt
- Benutzung nur für authentifizierte Benutzer und Geräte erlaubt
  nicht erfüllt
- eindeutige, benutzerorientierte Kostenabrechnung
  ???
- Vermeidung der einfachen Erstellung von Bewegungsprofilen
  ???

lesenswert:
Sicherheit im Funk-LAN (WLAN, IEEE 802.11)
BSI, Bonn 2002, http://www.bsi.bund.de

Lösungsansätze

- zusätzliche Verschlüsselung der Daten ist nötig
- Einsatz eines VPN (virtual private network)
  Realisierung per L2TP bzw. Ipsec
- Ipsec erfüllt die anforderungen bezügl.
  Integrität, Authentizität und Vertraulichkeit
- allerdings sind VPNs nicht das Nonplusultra
  für mobile Sicherheit, weil
  - VPNs empfindlich auf Unterbrechungen
    reagieren, auch auf kurzzeitige
  - durchschnittliche VPN-Server max. 30-50 Mbit/s
    Durchsatz vorweisen -> schnell erreicht
  - spezielle VPN-Clients auf den Endgeräten nötig

Fazit

- die existierenden Realisierungen mobiler Kommunikation sind unsicher
- im Mobilfunk wird nur ein Technikwechsel Abhilfe schaffen (UMTS ?)
- bei WLAN-Realisierungen muss der Datenstrom zusätzlich verschlüsselt werden (z.B. VPN)
- neue Normen versprechen Abhilfe
  IEEE 802.11i, 802.1x

Thüringen auf dem Weg in die Informationsgesellschaft

Bauhaus-Universität Weimar, Fakultät Medien
bernd.schalbe@medien.uni-weimar.de
www.uni-weimar.de/medien

Bauhaus-Universität Weimar
fakultät medien [faculty of media]